إصدار ASA 8.3: تجاوز MSS - يتعذر على عملاء HTTP الاستعراض إلى بعض مواقع الويب

المحتويات

المقدمة

يصف هذا المستند مشكلة تحدث عندما لا يمكن الوصول إلى بعض مواقع الويب من خلال جهاز الأمان القابل للتكيف (ASA) الذي يشغل الإصدار 8.3 أو برنامج أحدث.

يقدم إصدار ASA 7.0 العديد من تحسينات الأمان الجديدة، يكون أحدها التحقق من نقاط نهاية TCP التي تلتزم بالحد الأقصى لحجم المقطع (MSS) المعلن عنه. في جلسة TCP عادية، يرسل العميل حزمة SYN إلى الخادم، مع تضمين MSS ضمن خيارات TCP من حزمة SYN. يجب أن يتعرف الخادم، عند إستلام حزمة SYN، على قيمة MSS التي تم إرسالها بواسطة العميل ثم يرسل قيمة MSS الخاصة به في حزمة SYN-ACK. بمجرد إدراك كل من العميل والخادم لـ MSS الخاص بالآخر، لا يجب على أي من النظراء إرسال حزمة إلى الآخر أكبر من MSS الخاص به هذا النظير.

تم اكتشاف وجود عدد قليل من خوادم HTTP على الإنترنت لا تحترم MSS التي يعلن عنها العميل. وبعد ذلك، يرسل خادم HTTP حزم البيانات إلى العميل الأكبر من MSS المعلن عنها. قبل الإصدار 7.0، تم السماح بهذه الحزم من خلال ASA. ومع تضمين تحسين الأمان في إصدار 7.0، يتم إسقاط هذه الحزم بشكل افتراضي. تم تصميم هذا المستند لمساعدة المسؤول في تشخيص هذه المشكلة وتنفيذ حل بديل من Cisco في جهاز الأمان القابل للتكيف للسماح بالحزم التي تتجاوز MSS.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى جهاز الأمان القابل للتكيف (ASA) من Cisco الذي يشغل الإصدار 8.3 من البرنامج.

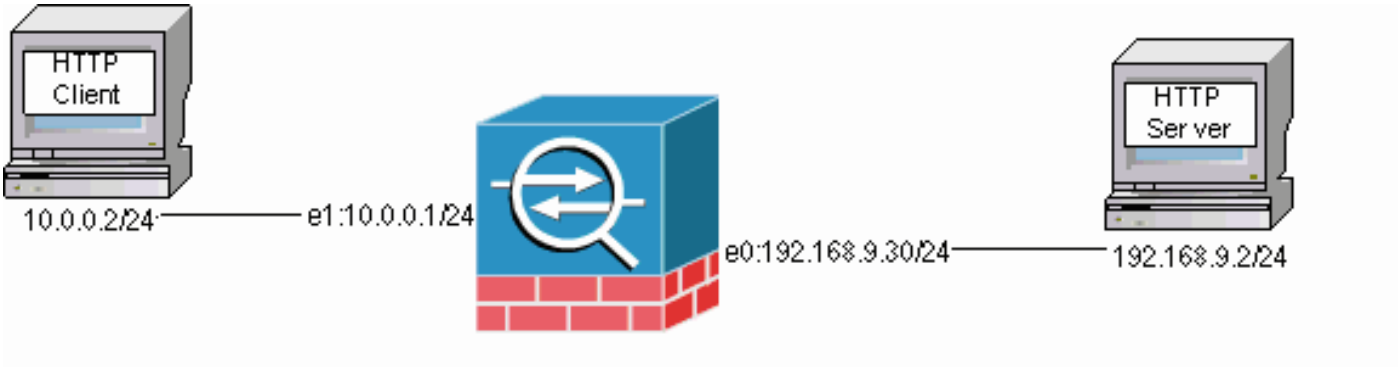
تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يقدم لك هذا القسم معلومات تكوين الميزات التي يصفها هذه المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين ASA 8.3

تتم إضافة أوامر التكوين هذه إلى التكوين الافتراضي ASA 8.3 للسماح لعميل HTTP بالاتصال بخادم HTTP.

تكوين ASA 8.3

```
ASA(config)#interface Ethernet0
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address 192.168.9.30 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface Ethernet1
ASA(config-if)#speed 100
ASA(config-if)#duplex full
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 10.0.0.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#object network Inside-Network
ASA(config-obj)#subnet 10.0.0.0 255.0.0.0
ASA(config)#nat (inside,outside) source dynamic Inside-Network interface
ASA(config)#route outside 0.0.0.0 0.0.0.0 192.168.9.2 1
```

استكشاف الأخطاء وإصلاحها

إذا لم يكن الوصول إلى موقع ويب معين من خلال ASA، أكمل الخطوات التالية لاستكشاف الأخطاء وإصلاحها. تحتاج أولا إلى التقاط حزم HTTP. لتجميع الحزم، يلزم معرفة عناوين IP ذات الصلة لخادم HTTP والعميل، بالإضافة إلى عنوان IP الذي تترجمه العميل إليه عندما يجتاز ASA.

في شبكة المثال، يتم تنزيل خادم HTTP في 192.168.9.2، ويتم معالجة عميل HTTP في 192.168.9.30 حيث ترك الحزم الواجهة الخارجية. 10.0.0.2، وتتم ترجمة عناوين عميل HTTP إلى عنوان Cisco لتجميع (ASA) من الجدار الناري للتكيف. يمكنك استخدام ميزة التقاط، فيمكن الحزم، أو يمكنك استخدام التقاط حزمة خارجي. إذا كنت تنوي استخدام ميزة التقاط مضمنة في الإصدار 7.0 الذي يسمح للمسؤول أيضا استخدام ميزة التقاط جديدة للمسؤول بالتقاط الحزم التي يتم إسقاطها بسبب خطأ TCP.

ملاحظة: تلتف بعض الأوامر في هذه الجداول على سطر ثان بسبب القيود المكانية.

1. قم بتحديد زوج من وقائع الوصول التي تعرف الحزم أثناء دخولها وخروجها من الواجهات الخارجية والداخلية.
2. مكنت التقاط سمة ل على حد سواء الداخلي والخارجي قارن. قم أيضا بتمكين التقاط للحزم التي تم تجاوز MSS الخاصة ب TCP.
3. امسح عدادات مسار الأمان السريع (ASP) على ASA.
4. قم بتمكين sysloing للمراقبة عند مستوى تصحيح الأخطاء الذي تم إرساله إلى مضيف على الشبكة.
5. ابدأ جلسة HTTP من عميل HTTP إلى خادم HTTP المثير للمشاكل، وتجمع إخراج syslog والمخرجات من هذه الأوامر بعد فشل الاتصال.**show capture-insideshow capture-outsideshow capture mss-capture**إظهار التقاط ASP**ملاحظة:** ارجع إلى رسالة سجل النظام رقم 419001 للحصول على مزيد من المعلومات حول رسالة الخطأ هذه.

الحل

قم بتنفيذ حل بديل الآن حيث تعلم أن ASA يسقط الحزم التي تتجاوز قيمة MSS التي يعلن عنها العميل. تذكر أنه قد ترغب في السماح لهذه الحزم بالوصول إلى العميل بسبب تجاوز سعة التخزين المؤقت المحتمل على العميل. إذا أخترت السماح لهذه الحزم من خلال ASA، فعليك متابعة إجراء الحل البديل هذا.

إطار عمل السياسة النمطية (MPF) هو ميزة جديدة في الإصدار 7.0 يتم استخدامه للسماح بهذه الحزم من خلال ASA. لم يتم تصميم هذا المستند لإجراء تفاصيل كاملة حول ميزة "حماية مستوى الإدارة (MPF)" ولكن بدلا من ذلك يشير إلى كيانات التكوين المستخدمة لحل المشكلة. ارجع إلى دليل التكوين ASA 8.3 للحصول على مزيد من المعلومات حول ميزة "حماية مستوى الإدارة (MPF)".

تتضمن نظرة عامة على الحل البديل تعريف عميل HTTP والخوادم عبر قائمة وصول. بمجرد تحديد قائمة الوصول، يتم إنشاء خريطة فئة ويتم تعيين قائمة الوصول إلى خريطة الفئة. ثم يتم تكوين خريطة TCP ويتم تمكين الخيار للسماح بالحزم التي تتجاوز MSS. بمجرد تحديد خريطة TCP وخريطة الفئة، يمكنك إضافتها إلى خريطة سياسة جديدة أو موجودة. يتم بعد ذلك تعيين خريطة نهج لنهج أمان. أستخدم الأمر **service-policy** في وضع التكوين لتنشيط خريطة سياسة بشكل عام أو على واجهة. وتتم إضافة معلمات التكوين التالية إلى قائمة التكوين 8.3 لجدار الأمان القابل للتكيف (ASA) من Cisco. بعد إنشاء خريطة نهج باسم "http-map1"، يضيف نموذج التكوين هذا خريطة الفئة إلى خريطة النهج هذه.

واجهة محددة: تكوين MPF للسماح بالحزم التي تتجاوز MSS

```
ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match access-list http-list2
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 interface outside
ASA#
```

وبمجرد وضع معلمات التكوين هذه في مكانها، يتم السماح بالحزم من 192.168.9.2 التي تتجاوز MSS المعلن عنها بواسطة العميل من خلال ASA. من المهم ملاحظة أن قائمة الوصول المستخدمة في خريطة الفئة مصممة لتحديد حركة المرور الصادرة إلى 192.168.9.2. يتم فحص حركة المرور الصادرة للسماح لمحرك الفحص باستخراج MSS من حزمة SYN الصادرة. إذا كانت هناك حاجة إلى تعديل SYN في الاعتبار، فإن الضروري تكوين قائمة الوصول مع وضع إتجاه SYN في الاعتبار. لذلك، يمكنك إستبدال بيان **قائمة الوصول** في هذا القسم ببيان أكثر انتشارا، مثل **قائمة الوصول http-list2 السماح ip any** أو **access-list http-list2 السماح tcp any** الذي يسمح بكل شيء. تذكر أيضا أن نفق VPN يمكن أن يكون بطيء إذا تم إستخدام قيمة كبيرة من TCP MSS. يمكنك تقليل TCP MSS لتحسين الأداء.

يساعد هذا المثال على تكوين حركة المرور الواردة والصادرة بشكل عام في ASA:

التكوين العام: تكوين MPF للسماح بالحزم التي تتجاوز MSS

```
ASA(config)#access-list http-list2 permit tcp any host 192.168.9.2
ASA(config)#
ASA#configure terminal
ASA(config)#
ASA(config)#class-map http-map1
ASA(config-cmap)#match any
ASA(config-cmap)#exit
ASA(config)#tcp-map mss-map
ASA(config-tcp-map)#exceed-mss allow
ASA(config-tcp-map)#exit
ASA(config)#policy-map http-map1
ASA(config-pmap)#class http-map1
ASA(config-pmap-c)#set connection advanced-options mss-map
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#service-policy http-map1 global
ASA#
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

كرر الخطوات الموجودة في قسم [أستكشاف الأخطاء وإصلاحها](#) للتحقق من أن تغييرات التكوين تفعل ما تم تصميمها للقيام به.

حجز اتصال من Syslog

```
%ASA-6-609001: Built local-host inside:10.0.0.2
%ASA-6-609001: Built local-host outside:192.168.9.2
%ASA-6-305011: Built dynamic TCP translation from inside:10.0.0.2/58798
               to outside:192.168.9.30/1025
%ASA-6-302013: Built outbound TCP connection 13 for outside:192.168.9.2/80
               (192.168.9.2/80) to inside:10.0.0.2/58798 (192.168.9.30/1025)
%ASA-5-304001: 10.0.0.2 Accessed URL 192.168.9.2:/

%ASA-6-302014: Teardown TCP connection 13 for outside:192.168.9.2/80 to
               inside:10.0.0.2/58798 duration 0:00:01 bytes 6938 TCP FINs

!--- The connection is built and immediately !--- torn down when the web content is retrieved.
```

إخراج من أوامر العرض من اتصال ناجح

```
ASA#
ASA#show capture capture-inside
21 packets captured
   1: 09:16:50.972392 10.0.0.2.58769 > 192.168.9.2.80: S
      751781751:751781751(0)
   win 1840 <mss 460,sackOK,timestamp 110313116 0,nop,wscale 0>

 !--- The advertised MSS of the client is 460 in packet #1. However, !--- with th workaround in place,
packets 7, 9, 11, 13, and 15 appear !--- on the inside trace, despite the MSS>460. 2: 09:16:51.098536
192.168.9.2.80 > 10.0.0.2.58769: S 1305880751:1305880751(0) ack 751781752 win 8192 <mss 1380> 3:
09:16:51.098734 10.0.0.2.58769 > 192.168.9.2.80: . ack 1305880752 win 1840 4: 09:16:51.099009 10.0.0.2.
> 192.168.9.2.80: P 751781752:751781851(99) ack 1305880752 win 1840 5: 09:16:51.228412 192.168.9.2.80 >
10.0.0.2.58769: . ack 751781851 win 8192 6: 09:16:51.228641 192.168.9.2.80 > 10.0.0.2.58769: . ack 7517
win 25840 7: 09:16:51.236254 192.168.9.2.80 > 10.0.0.2.58769: . 1305880752:1305882112(1360) ack 7517818
25840
   8: 09:16:51.237704 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305882112 win 4080
   9: 09:16:51.243593 192.168.9.2.80 > 10.0.0.2.58769: P
      1305882112:1305883472(1360) ack 751781851 win 25840
  10: 09:16:51.243990 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305883472 win 6800
  11: 09:16:51.251009 192.168.9.2.80 > 10.0.0.2.58769: .
      1305883472:1305884832(1360) ack 751781851 win 25840
  12: 09:16:51.252428 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305884832 win 9520
  13: 09:16:51.258440 192.168.9.2.80 > 10.0.0.2.58769: P
      1305884832:1305886192(1360) ack 751781851 win 25840
  14: 09:16:51.258806 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305886192 win 12240
  15: 09:16:51.266130 192.168.9.2.80 > 10.0.0.2.58769: .
      1305886192:1305887552(1360) ack 751781851 win 25840
  16: 09:16:51.266145 192.168.9.2.80 > 10.0.0.2.58769: P
      1305887552:1305887593(41) ack 751781851 win 25840
  17: 09:16:51.266511 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887552 win 14960
  18: 09:16:51.266542 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887593 win 14960
  19: 09:16:51.267320 10.0.0.2.58769 > 192.168.9.2.80: F
      751781851:751781851(0) ack 1305887593 win 14960
  20: 09:16:51.411370 192.168.9.2.80 > 10.0.0.2.58769: F
      1305887593:1305887593(0) ack 751781852 win 8192
  21: 09:16:51.411554 10.0.0.2.58769 > 192.168.9.2.80: .
      ack 1305887594 win 14960
21 packets shown
ASA#
ASA#
ASA#show capture capture-outside
21 packets captured
```

```
   1: 09:16:50.972834 192.168.9.30.1024 > 192.168.9.2.80: S
      1465558595:1465558595(0) win 1840 <mss 460,sackOK,timestamp
      110313116 0,nop,wscale 0>
   2: 09:16:51.098505 192.168.9.2.80 > 192.168.9.30.1024:
      S 466908058:466908058(0) ack 1465558596 win 8192 <mss 1460>
   3: 09:16:51.098749 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466908059 win 1840
   4: 09:16:51.099070 192.168.9.30.1024 > 192.168.9.2.80: P
      1465558596:1465558695(99) ack 466908059 win 1840
   5: 09:16:51.228397 192.168.9.2.80 > 192.168.9.30.1024: .
      ack 1465558695 win 8192
   6: 09:16:51.228625 192.168.9.2.80 > 192.168.9.30.1024: .
      ack 1465558695 win 25840
   7: 09:16:51.236224 192.168.9.2.80 > 192.168.9.30.1024: .
      466908059:466909419(1360 ack 1465558695 win 25840
   8: 09:16:51.237719 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466909419 win 4080
   9: 09:16:51.243578 192.168.9.2.80 > 192.168.9.30.1024: P
      466909419:466910779(1360) ack 1465558695 win 25840
  10: 09:16:51.244005 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466910779 win 6800
  11: 09:16:51.250978 192.168.9.2.80 > 192.168.9.30.1024: .
      466910779:466912139(1360) ack 1465558695 win 25840
  12: 09:16:51.252443 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466912139 win 9520
  13: 09:16:51.258424 192.168.9.2.80 > 192.168.9.30.1024: P
      466912139:466913499(1360) ack 1465558695 win 25840
  14: 09:16:51.258485 192.168.9.2.80 > 192.168.9.30.1024: P
      466914859:466914900(41) ack 1465558695 win 25840
  15: 09:16:51.258821 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466913499 win 12240
  16: 09:16:51.266099 192.168.9.2.80 > 192.168.9.30.1024: .
      466913499:466914859(1360) ack 1465558695 win 25840
  17: 09:16:51.266526 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914859 win 14960
  18: 09:16:51.266557 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914900 win 14960
  19: 09:16:51.267335 192.168.9.30.1024 > 192.168.9.2.80: F
      1465558695:1465558695(0) ack 466914900 win 14960
  20: 09:16:51.411340 192.168.9.2.80 > 192.168.9.30.1024: F
      466914900:466914900(0) ack 1465558696 win 8192
  21: 09:16:51.411569 192.168.9.30.1024 > 192.168.9.2.80: .
      ack 466914901 win 14960
21 packets shown
ASA#
ASA(config)#show capture mss-capture
0 packets captured
0 packets shown
ASA#
ASA#show asp drop

Frame drop:

Flow drop:
ASA#

!--- Both the show capture mss-capture and the show asp drop !--- commands reveal that no packets are
dropped.
```

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك أجهزة الأمان المعدلة (ASA) من Cisco)
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).